УДК 532.517

ПРОБЛЕМИ ПОБУДОВИ СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ НА ОБ'ЄКТАХ, ЩО ПОТРЕБУЮТЬ ВИСОКОГО РІВНЯ БЕЗПЕКИ

А. А. Кулько[1, a], О. Д. Василенко[1]

[1] *Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Фізико-технічний інститут*

Анотація

Для побудови ефективної системи відеоспостереження на об'єктах, що потребують високого рівня безпеки (аеропорт міжнародного значення, залізничний вокзал, торговий центр, стадіон, тощо) необхідно визначити алгоритм її побудови в якому будуть враховані усі можливі загрози та атаки у кожному конкретному випадку. Цей матеріал призначений для попереднього розгляду проблем, що можуть виникати на території міжнародного аеропорту.

Ключові слова: аеропорт, відеоспостереження, загрози та атаки

Вступ

На даний час площі, що займають міжнародні аеропорти доходять до розмірів невеликих населених пунктів, між терміналами або виходами до літаків якого транспортне сполучення може бути, як автобусне, так і залізничне у виді аеропортної сітки метро, що ускладнює контроль та підтримку рівня безпеки на території аеропорту.

За останні роки кількість атак у місцях масового скупчення людей стрімко зросла, що обумовлено нестабільною політичною ситуацією у світі. Зазвичай об'єктами на яких наявна загроза є стадіони та транспортні сполучення (залізничні вокзами, лінії метро, аеропорти, стадіони, тощо).

У зв'язку з цим зросла потреба у сучасних засобах та системах своєчасного виявлення та ідентифікації загроз. Відомо, що одним з ефективних засобів виявлення та ідентифікації атак є система відеоспостереження, що особливо стосується об'єктів, де наявна скупченість людей та транспорту. Для забезпечення захисту аеропортів (аеродромів) або провайдера аеронавігаційного обслуговування застосовується відеоспостереження, патрулювання та інші заходи безпеки, у тому числі з метою виявлення осіб з підозрілою поведінкою, визначення уразливих місць, які можуть бути використані для здійснення акту незаконного втручання. [1]

Будь яке відеоспостереження виконується за допомогою раціонального розташування відповідної кількості відео камер. Також є важливим розглянути всі напрямки та всі точки можливого забезпечення відеоспостереження, де воно потрібно і як воно буде застосовуватися, а також визначення кількості та номенклатури камер відеоспостереження.

[a] kulko.andrii@gmail.com

1. Загрози безпеки аеропорту

Загальний поділ наявних загроз на території аеропорту може складатись з чотирьох чинників:

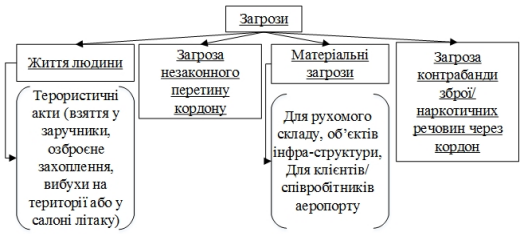

Рис. 1. Структура поділу загроз

До загроз життю людини віднесено можливі терористичні акти, наприклад масове озброєне захоплення, взяття у заручники пасажирів або робітників аеропорту, вибухи на території аеропорту, тощо.

До загроз матеріальній частині відносяться крадіжки особистих речей, викрадення авто зі стоянки аеропорту, пошкодження транспортної складової аеропорту та інфраструктури аеропорту.

Для визначення зон, в яких можливі загрози можуть перетворитися в реальні атаки, розглянемо можливу мету зловмисника (терориста) Метою порушника безпеки аеровокзалу є непомітне для служби безпеки проникнення на об'єкт з метою досягнення поставлених цілей.

Можливі цілі порушника:

1) Скоєння терористичного акту методом захоплення заручників або принесення жертв.
2) Крадіжка особистих речей.
3) Провезення заборонених засобів та предметів.
4) Пошкодження технічного стану авіа рухомого складу та інфраструктури аеропорту.
5) Незаконний перетин кордону.

При цьому формування захисту від атак повинно базуватись на визначенні моделі порушника відносно

конкретного об'єкту. Згідно [2] модель порушника це абстрактний формалізований або неформалізований опис дій порушника, який відображає його практичні та теоретичні можливості, апріорні знання По відношенню до об'єкту порушники можуть бути внутрішніми, тобто з числа співробітників (обслуговуючий персонал або співробітник служби безпеки) або зовнішніми (не мають відношення до роботи аеропорту).

З урахуванням вищезазначеного необхідно при побудові системи відео спостереження розглядати можливість атак від усіх видів порушників.

2. Зони можливих атак об'єкту

Умовний поділ території аеропорту на зони може бути представлений з чотирьох складових:

Рис. 2. Структура поділу території аеропорту на зони

Територію аеропорту можна умовно поділити на внутрішню та зовнішню територію. Внутрішньою зоною є будівля терміналу аеропорту. Зовнішньою зоною спостереження є прилегла інфраструктура, що не знаходиться на території контрольованої зони (паркінг автомобілів клієнтів аеропорту, зупинки громадського транспорту, зони для проходу людей). Зовнішня контрольована зона – обмежена парканом, у якій розташовані злітно-посадкові смуги, ангари для стоянки/обслуговування літаків, місця тимчасової стоянки/обслуговування/очікування на зліт літаків. [3] Зоною найбільшої загрози є внутрішня зона терміналу аеропорту.

Послідовність розташування зон, під час прибуття літака до аеропорту:

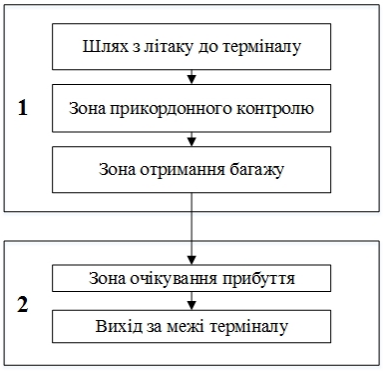

Рис. 3. Структура проходження зон пасажирами під час прибуття

З наведеної структури видно, що виділення другої зони є територію з найбільшим скупченням людей відповідно з найвищим рівнем загроз. Виділення першої зони — територія з нижчим рівнем загроз, оскільки пасажири літака, що прибув, пройшли попередні заходи безпеки у іншому аеропорту звідки прибув літак. Однак, зберігається загроза незаконного перетину кордону.

Послідовність проходження зон пасажирами, під час відправлення літака з аеропорту:

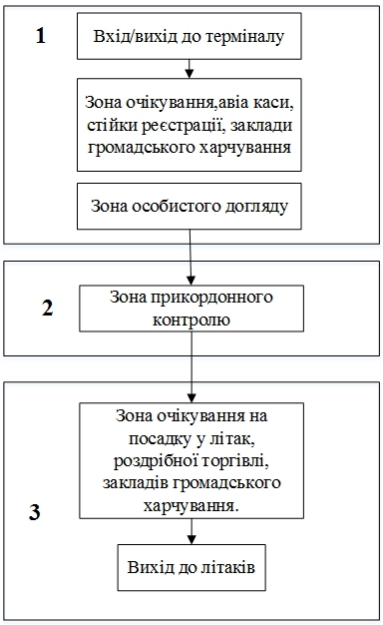

Рис. 4. Структура проходження зон пасажирами під час відправлення

Як видно з наведеної структури, виділення першої зони є територію з найбільшим скупченням людей відповідно з найвищим рівнем загроз.

Друга зона є зоною прикордонного контролю, куди мають доступ тільки пасажири, що пройшли попередні заходи безпеки на межі першої та другої виділених зон. Відповідно рівень загроз значно менший, ніж у першій виділеній зоні.

Виділення третьої зони — територія з найнижчим рівнем загроз (після процедури особистого догляду). Зоною найбільшої загрози є внутрішня зона терміналу аеропорту.

3. Попередніми рекомендаціями, щодо розташування камер відео спостереження є:

— Рівень загроз в зоні. У відповідності до рівня загрози у зоні, де встановлюється камера відеоспостереження, визначається їх кількість, якість та характеристики, що використовуються для виявлення можливих атак. [3] У сукупності зон під номером 1 (Рис.3) слід застосовувати камери з функцією ідентифікації обличь, порівняння їх з базою даних розшуку,виявлення полишених речей, великого скупчення людей, що підвищує рівень загрози у даний момент часу, оскільки рівень загроз цієї зони – найвищий.

— Рівень незаконного перетину кордону. У зонах митного контролю підвищений ризик незаконного перетину кордону, тому кількість камер на одне прикордонне віконце мінімум дві — одна камера загального плану виду зверху, друга — камера, що

безпосередньо розташована на рівні обличчя людини середнього зросту (170 см).

— Рівень загроз проникнення в контрольовану зону. У зовнішніх зонах спостереження та контрольованих для терміналу слід використовувати камери, що адаптивні до зміни освітлення або його відсутності, зміни погодних умов. На в'їзді в контрольовану зону необхідно встановлювати камери, що можуть ідентифікувати номерні знаки автомобілей, обличчя людей та мають можливість прослідкувати за траекторією пересування об'єкту виявлення. Як видно з наведених структур для нагляду за різними зонами необхудні різні за номенклатурою камери, як для денного (штучного) світла, так і для нічного спостереження (зона паркінгу, стоянок літаків, злітно-посадкових смуг).

Висновки

У данній роботі розглянуті можливі загрози безпеки на об'єкті рівня міжнародного аеропорту, їх структурований поділ зображено на Рис.1.

Представлено структурований поділ об'єкту на зони та відповідно до рівня загроз (Рис.2-4).базуючись на правилах організації системи контролю доступу та внутрішньооб'єктового режиму в суб'єктах авіаційної діяльності та на об'єктах цивільної авіації України. [1]

Розроблено рекомендації з використанння та встановлення камер відеоспостереження..

Перелік використаних джерел

1. Правила організації системи контролю доступу та внутрішньооб'єктового режиму в суб'єктах авіаційної діяльності та на об'єктах цивільної авіації України Закон України - VIII, Додатку 17 «Безпека. Захист цивільної авіації від актів незаконного втручання» до Конвенції про міжнародну цивільну авіацію. — 2017. — P. 47.
2. Біленчук П. Д., Романюк Б. В., Цимбалюк В. С. Комп'ютерна злочинність. – К. Атака,. — 2002. — P. 240.
3. Правила організації системи контролю доступу та внутрішньооб'єктового режиму в суб'єктах авіаційної діяльності та на об'єктах цивільної авіації України Закон України - VIII, Додатку 17 «Безпека. Захист цивільної авіації від актів незаконного втручання» до Конвенції про міжнародну цивільну авіацію. — 2017. — P. 62.